IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

K. MIZRA, LLC,	)	
	)	
Plaintiff,	)	**C.A. NO. 6:20-CV-01031-ADA**
	)	
v.	)	
	)	**PUBLIC VERSION**
CISCO SYSTEMS, INC.	)	
	)	
Defendant.	)	
	)	

DEFENDANT CISCO SYSTEMS, INC.'S OPENING BRIEF IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT OF NONINFRINGEMENT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

I. INTRODUCTION

K.Mizra's infringement claim fails as a matter of law. As Cisco has briefed elsewhere, the remaining asserted patent, U.S. Patent No. 8,234,705, is invalid, and a licensing agreement bars K.Mizra's claims. ECF Nos. 49, 82, 113. But even if K.Mizra could overcome those obstacles (it cannot), the victory would be pyrrhic because its infringement theory fails on multiple grounds: First, based on the undisputed record, including the testimony of K.Mizra's own expert, K.Mizra cannot show that Cisco or any Cisco customer directly infringes the '705 Patent. Without proof of direct infringement *by anyone*, K.Mizra obviously cannot prove indirect infringement either. Second, K.Mizra has no evidence of intent to induce infringement. Finally, K.Mizra has no evidence that Cisco products have any connection with the required trusted platform module ("TPM") claim limitation. Nor is there any evidence that Cisco products employ the DNS redirect the claims require. For each of these reasons, the undisputed factual record shows that Cisco does not infringe the '705 Patent. The Court should grant summary judgment of noninfringement.

II. UNDISPUTED FACTS

The Asserted Patent. The '705 Patent is called "Contagion Isolation and Inoculation." Ex. A ('705 Patent) at [54]. It has three independent claims that are "essentially identical" in substantive scope. Ex. B (Clark Noninfringement Report) ¶ 47; Ex. C (Cole Infringement Report) ¶ 79; Ex. D (Medvidovic Dep. Excerpts) at 66:21-67:3. These claims cover a method (claim 1); a system with a processor configured to perform the identical method (claim 12); and a computer program product "embodied in a non-transitory computer readable medium and comprising instructions for" the same method (claim 19). The method common to all the claims is for protecting a computer network against potentially dangerous host devices. Ex. A at cls. 1, 12, 19.[1]

[1] K.Mizra also asserts dependent claim 9, which depends from claim 1, and dependent system claim 16, which depends from claim 12. The dependent limitations are not at issue in this motion.

For purposes of this motion, the following aspects of the claimed approach are relevant and undisputed:

When host devices (such as computers belonging to users) attempt to access a protected network, the invention determines whether the host presents a security threat. Ex. A at [57], 3:8-45. The claims recite specific threats to check for, a specific way to perform the check, and, if the host's security state is inadequate, a specific way to quarantine and remediate the host:

Threats to check for: The claims require the network to check for an "attestation of cleanliness" from the host that assures the network either that the host is not infested with malicious code, or viruses or worms, Ex. E (Cole Dep.) at 84:15-20, or that the host has ascertained the presence of a software patch or patch level (meaning, a software update that fixes a vulnerability or the version number of such an update), Ex. E at 100:19-101:21.[2]

How to check: As part of the security evaluation, all claims require the following limitation: "contacting a trusted computing base associated with a trusted platform module within the first host."[3] The Court has construed "trusted platform module" to mean a "secure cryptoprocessor that can store cryptographic keys and that implements the Trusted Platform Module specification from the Trusted Computing Group." ECF No. 46 at 1. The attestation of cleanliness must come from the trusted computing base associated with a TPM within the first host. Ex. A at cl. 1, 19:60-65, cl. 12, 21:5-10, cl. 19, 22:20-25; *see also* Ex. D at 76:24-77:19.

***Quarantine and remediation*:** If the host fails to provide a cleanliness assertion, the network quarantines the host using a specific procedure. Namely, when the host computer sends a

[2] *See also* Ex. A at cl. 1 ("the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host").
[3] Ex. A at cl. 1, 19:60-62, cl. 12, 21:5-8, cl. 19, 22:20-22.

request for a web server, the network does one of the following:

(i) if the host requests anything other than a remediation website that provides data for remedying the insecure condition (such a software patch update or an antivirus program), the network reroutes the host to a quarantine server that serves a quarantine notification page. The network must perform redirection by answering a Domain Name Server ("DNS") request with the IP address of the quarantine server (*i.e.*, "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server"), rather than the IP address for a non-remediation site the host computer requested.[4] Other types of redirection do not meet the claim.

(ii) if the host requests a remediation website, the network does not redirect but simply permits the host to communicate with the remediation website.[5]

The Accused Combination. K.Mizra does not assert that any single Cisco product infringes any asserted claim. Rather, it alleges that two different Cisco software products that are sold separately, Identity Services Engine ("ISE") and AnyConnect Secure Mobility Client ("AnyConnect"), infringe if used together in just the right way.[6] In particular, its theory requires a customer to purchase and deploy both products together, to opt for the highest ("Premier")[7] licensing levels, to then have a network administrator select certain distinct settings, and all to protect and enable network access by end users' individual computers running both AnyConnect and the Microsoft Windows 10 or 11 operating system (which Cisco doesn't sell and which its products do not require). Ex. E at 25:16-20, 26:19-25, 27:14-28:19.

---

[4] Ex. A at cl. 1, 20:14-17, cl. 12, 21:27-30, cl. 19, 22:41-43.
[5] Ex. A at cl. 1, 20:5-21 ("in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host").
[6] This product is now called "Cisco Secure Client"; for simplicity, we refer to it as "AnyConnect."
[7] "Apex" and "Premier" refer to the same license level; "Apex" has been renamed "Premier." To minimize confusion, we refer to both as "Premier."

The accused feature is the "posture check" that ISE may be configured to perform on individual computers attempting to connect to a network—but only when carried out in combination with AnyConnect's "ISE Posture" module, and only with certain settings. In particular, K.Mizra accuses a configuration and procedure whereby AnyConnect is loaded on a host device (individual computer), attempts to connect to a network running ISE, and ISE prompts AnyConnect to perform the posture check where the network administrator has configured the following settings: (i) set the posture policy to require that the host computer check for a current infestation or a software patch or patch level,[8] and, if the host fails the check, set ISE to (ii) redirect any web request from the host to a quarantine server that allows access to remediation, but to (iii) skip the redirection step if the host's web request was for a remediation host set up to provide data that can be used to remedy the issue that caused the host device to fail posture.[9]

ISE alone does not infringe. Neither does AnyConnect. *See* Ex. C ¶ 22, Ex. F (Appendix C to Cole Infringement Report) at 1; Ex. B ¶¶ 47-123. Similarly, ISE and AnyConnect deployed together but at licensing tiers lower than Premier are not accused because lower license tiers do not possess the accused functionality. Ex. E at 221:17-22; *see* Ex. C ¶ 84.

And the Cisco products in the accused combination do not even allegedly contain a key limitation—the trusted platform module. For the TPM limitation, K.Mizra relies on Microsoft

[8] Ex. A at cl. 1, 19:65-20:4 ("the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host").

[9] Ex. A at cl. 1, 20:5-21 ("when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by … receiving a service request sent by the first host … and in the event the service request comprises a DNS query, *providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host*" (emphasis added)).

product literature stating that computers running its Windows 10 and Windows 11 operating systems must contain a TPM. Ex. F at 31, 32-42; *see* Ex. E at 43:17-44:7. There is no evidence, however, that a TPM on those computers interacts with the accused Cisco products or is involved in the accused functionality. K.Mizra has neither reviewed, identified, nor attempted to introduce any Microsoft source code. Ex. E at 143:12-22.

III. LEGAL STANDARD

"Summary judgment must be rendered when the pleadings, the discovery and disclosure materials on file, and any affidavit show that there is no genuine dispute as to any material fact and that the moving party is entitled to a judgment as a matter of law." *VLSI Tech. LLC v. Intel Corp.*, No. 1:19-CV-977-ADA, 2021 WL 2773013, at *2 (W.D. Tex. Apr. 12, 2021). The Court must "view all inferences drawn from the factual record in the light most favorable to the nonmoving party" and may not make credibility determinations or weigh the evidence. *Id.* But mere "conclusory allegations" are not enough to defeat summary judgment. A party opposing summary judgment "is required to identify specific evidence in the record and to articulate the precise way that evidence supports their claim." *Id.*

IV. ARGUMENT

A. K.Mizra's infringement claims fail for lack of proof that anyone has ever assembled or used the Accused Combination in the claimed configuration.

K.Mizra cannot establish direct infringement—by *anyone*. Because K.Mizra has no proof that anyone, let alone Cisco or any of its customers, directly infringes, all of its infringement claims—direct and indirect—fail as a matter of law.

1. Cisco does not directly infringe.

It is undisputed that Cisco does not directly infringe the method claims (claim 1). K.Mizra has not tried to show that Cisco or someone acting under Cisco's control or direction performs

each step of the claimed method. *See, e.g.*, *ESW Holdings, Inc. v. Roku, Inc.*, No. 6-19-CV-00044-ADA, 2021 WL 1069047, at *2 (W.D. Tex. Mar. 18, 2021) ("direct infringement occurs where all the steps of a claimed method are performed by or attributable to a single entity") (cleaned up). K.Mizra's theory is that Cisco sells the ISE and AnyConnect products to customers who then allegedly perform the method to protect their networks. Ex. E at 25:16-20, 26:19-25, 27:14-28:19. K.Mizra admits that Cisco neither puts the products into use itself, nor controls its customers' use of its product, nor contracts with its customers to require that they perform the steps K.Mizra accuses of infringing. Ex. E at 29:1-37:4. Therefore, Cisco cannot be a direct infringer of claim 1 or its dependents.

Nor does Cisco directly infringe the "configured to" and "computer program product" claims. To the extent K.Mizra and its expert seek to advance the theory that "mere capability" of being configured and used in this fashion could suffice, that is not the law. To establish direct infringement of claim 12, which requires a system with a processor "configured to" perform the identical method as claim 1, K.Mizra must prove that Cisco makes, uses or sells the accused products in the recited configuration. It is not enough that a product is merely "capable of" the claimed configuration. *Ball Aerosol and Specialty Container, Inc. v. Limited Brands, Inc.*, 555 F.3d 984, 994-95 (Fed. Cir. 2009) (where claim language recites a specific configuration, a product that is merely reasonably capable of being put in that configuration does not infringe absent proof it was actually put in that configuration); *ACCO Brands, Inc. v. ABA Locks Mfr. Co.*, 501 F.3d 1307, 1313 (Fed. Cir. 2007) (rejecting a "reasonably capable" standard for direct infringement and holding that infringement requires "specific instances of direct infringement or that the accused device necessarily infringes the patent in suit"). Likewise, to prove direct infringement of Claim 19 (a computer program product "comprising computer instructions for" performing the same

method), K.Mizra must prove Cisco's product is "programmed or otherwise configured, *without modification*, to perform the claimed function when in operation." *INVT SPE LLC v. ITC*, 46 F.4th 1361, 1365 (Fed. Cir. 2022) (emphasis added); *see id.* at 1376.

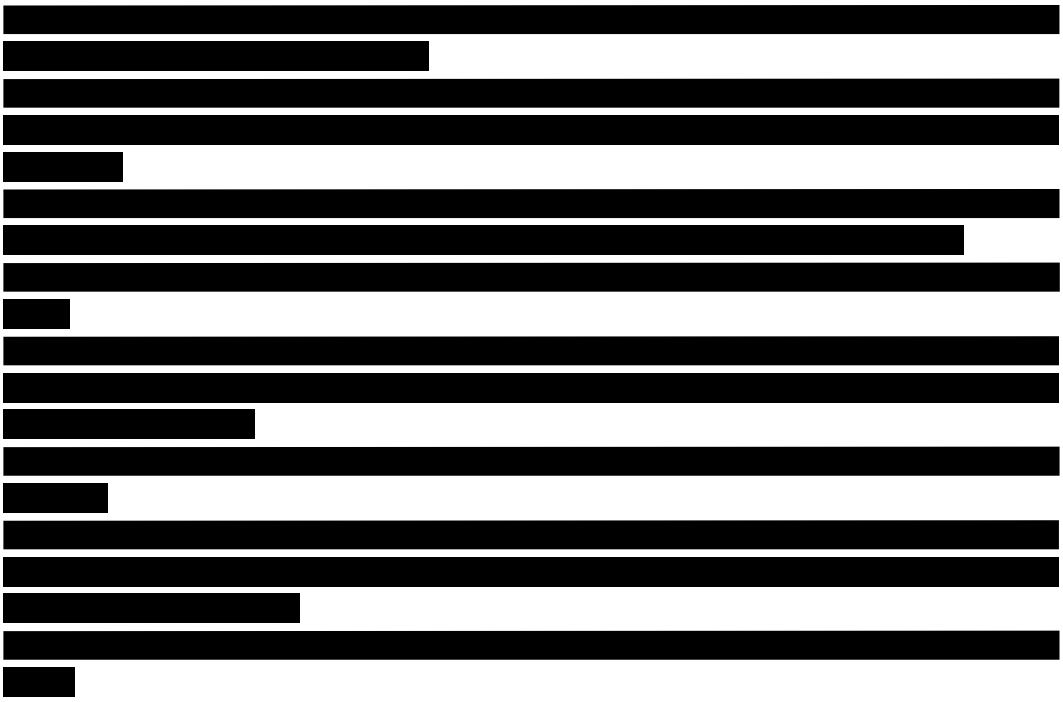
It is undisputed that Cisco does not make, use, or sell a system with the claimed configuration or programmed to, without modification, perform the method. To create either the accused system or the accused computer instructions, some entity running a network must (1) purchase the Premier license level of ISE and install it on the network, (2) instruct individual users (*e.g.*, the entity's employees or members) to use a client computer running the Windows 10 or 11 Operating System (a Microsoft product, which Cisco does not sell), (3) purchase, and install or instruct individual users to install, the Premier level of AnyConnect on that Windows device, and (4) set up ISE with the specific security policy, quarantine and remediation options required by the claims. This is not just Cisco's position; it is also K.Mizra's description of what the accused combination requires. Ex. E at 221:17-22 (both ISE Premier and AnyConnect Premier needed); Ex. F at 31-42 (Windows 10/11 device supplies TPM); Ex. E at 96:2-7, 96:8-19; 97:22-98:9, 204:12-207:15, 171:21-172:5, 172:13-173:15, 187:25-188:24 (acknowledging that network administrator selects settings for security policy, quarantine and remediation).

Any direct infringement theory fails because Cisco itself does not perform these acts and at a minimum because Cisco's products do not contain a necessary component identified by K.Mizra: a Windows 10 or 11 operating system running on a device containing a trusted platform module. Ex. E at 37:5-20 (K.Mizra not asserting that Cisco sells such devices); Ex. F at 31, 32-42. *See, e.g., Synchronoss Technologies, Inc. v. Dropbox, Inc.*, 987 F.3d 1358, 1368 (Fed. Cir. 2021) (where claims required hardware, the accused infringer did not "make" the claimed system since it did not provide any hardware, only software the customers used on their hardware, and therefore

did not provide the complete claimed invention). Under K.Mizra's theory, someone other than Cisco supplies a required component of the system—namely, the client device running Windows 10/11 and allegedly containing a trusted platform module. Thus, as a matter of law, K.Mizra cannot prove that Cisco directly infringes.

2. K.Mizra cannot prove that anyone else has directly infringed.

Prevailing on any theory of indirect infringement would require K.Mizra to show, at minimum, that someone other than Cisco, such as a Cisco customer, has directly infringed. It cannot do so. Its expert Dr. Cole does not even assert, much less show, direct infringement by any customer or group of customers:



Ex. E at 42:24-44:7.

K.Mizra's "evidence" of underlying direct infringement is thus not just weak; K.Mizra concedes it is entirely missing. That alone is sufficient to dispose of this case. And as explained below, its expert made other, further concessions that also defeat any theory of direct infringement.

K.Mizra has no evidence that anyone has performed, or configured or programmed a

system to perform, any of the customer-selected steps of the claimed method, nor put together a system containing ISE, AnyConnect, and the claimed trusted platform module. Each of these concessions standing alone is also, and independently, fatal to K.Mizra's case.

[1] Customer-selected step 1—the security policy: *"the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host."*

It is undisputed that Cisco's customer, when deploying ISE, chooses both whether to use posture and the security policy that the posture check enforces. Ex. E at 6:2-7, 96:8-19; 97:22-98:9; Ex. F at 45 ("posture defines the state of compliance with *the company's* security policy") (emphasis added); *id.* at 24 ("posture conditions customizable"). The customer can set the policy to check for, among other things, the latest operating system patch, antivirus and anti-spyware packages with current definition file variables (version, date, etc.), anti-malware packages, particular registry settings, patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, the presence of an application or of USB-attached media, a particular file, and/or other posture conditions. Ex. F at 54; Exhibit 5 to Ex. E at 21; Ex. E at 98:14-99:5, 121:13-122:8. K.Mizra has not identified any default or required conditions an ISE customer must include in the security policy. Ex. E at 99:1-100:17, 130:17-131:20; Ex. F at 5-14, 50-54.

Because there are numerous options and no required conditions, the customer's chosen settings determine whether the security policy could even arguably satisfy the claim limitation. And K.Mizra has no evidence of what particular security policy any of Cisco's customers choose. Ex. E at 112:22-113:18. To the contrary, its expert freely concedes that customers can select policies that check for things *other than* the software patch/patch level or current infestation that the asserted claims require checking. *See* Ex. E at 102:16-104:3 (policy need not check for software patch or patch level), 109:12-110:25 (policy that checks for whether the host's disk is encrypted,

whether the host has mobile PIN-lock, and whether any USB device is attached to it is not checking for current infestation), 125:3-126:9 (file-check condition can be set to check for any file and need not check for a software patch or patch level, or a current infestation).[10]

[2] Customer-selected step 2—the containment action: ***"quarantining the first host, including by … receiving a service request sent by the first host, … and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server … if a host name that is the subject of the DNS query is not associated with a remediation host… and … permitting the first host to communicate with the remediation host.***"

K.Mizra likewise has no evidence of any particular Cisco customer choosing, as a containment action, to quarantine the first host by redirecting it to a quarantine server that allows access to a remediation site. Ex. E at 222:22-223:6. Its expert concedes that the customer can set up the network to simply reject the request, or to quarantine the host *without* the claimed redirection to a special quarantine server that provides limited access for remediation. Ex. F at 62

[redacted] Ex. E at 205:7-9 [redacted] 204:16-207:15.

[3] Customer-selected step 3—the redirection: ***"providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host."***

Even if a customer were to select a policy that quarantines a host computer while allowing limited access to remediation sites, it need not do so in the manner the asserted claims specify. The claims recite that if the host fails the security policy, the network redirects any web request from the host *if it is not* a request for a remediation site. Thus, if the host *does* request a remediation site, the claims specify that redirecting to a quarantine server does not occur. K.Mizra's infringement expert conceded that Cisco's customers can simply set up the system to redirect *all* web requests

[10] K.Mizra has no evidence that AnyConnect is capable of checking for an infestation (it is not).

to a quarantine server, which, in turn, may provide links for navigating to remediation. Indeed, he characterized that noninfringing setting as the "typical way it's done." Ex. E at 182:6-13. And he admitted that his report shows no examples of the required configuration where the host requests a remediation site and is never redirected to quarantine. Ex. E at 180:17-183:4, 183:5-184:11. Yet again, K.Mizra has no evidence of any Cisco customer or set of customers choosing the accused option. Ex. E at 222:13-21.

[4] Customer-selected step 4—the trusted platform module: "*contacting a trusted computing base associated with a trusted platform module within the first host.*"

Finally, there is no evidence that any Cisco customers (such as companies that purchase ISE to run on their networks) requires their end users (e.g., their employees) to purchase Windows 10 or 11 devices containing a TPM, as opposed to another version of Windows or an Apple or Linux operating system—none of which require a TPM and none of which are accused. Cisco does not even allegedly require Windows 10/11. Ex. H (AnyConnect Guide) at 2 (cited in Dr. Cole's Report, Ex. C ¶ 82, and showing that AnyConnect supports numerous operating systems). K.Mizra concedes it has no evidence of any specific users who use ISE and AnyConnect with Windows 10 or 11, nor any data on the number who do so, if any. Ex. E at 43:17-44:7.

K.Mizra's infringement theory thus fails on its own terms, for lack of proof. Even if K.Mizra were right about what satisfies the claim limitations—and it is not, as explained below—it has no evidence and cannot prove that anyone has made, used, or even possessed the accused combination of products configured or programmed as K.Mizra contemplates. That is fatal to K.Mizra's entire case. Capability of infringing is not enough. *Ball Aerosol*, 555 F.3d at 994-95. K.Mizra needs, and doesn't have, evidence of "specific instances of direct infringement or that the accused device necessarily infringes the patent in suit." *ACCO Brands*, 501 F.3d at 1313; *see also ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 521 (Fed. Cir. 2012) (where plaintiff did not

present any evidence at trial that at least one user actually used the accused systems to perform the claimed method step, no reasonable jury could find the claim infringed).

B. Any attempt to claim indirect infringement fails for additional reasons.

There is no need to go further, because Cisco cannot be liable for indirect infringement absent proof that Cisco's actions led to direct infringement by another actor. *Dynacore Holdings Corp. v. U.S. Philips Corp.*, 363 F.3d 1263, 1274 (2004); *BillJCo, LLC v. Apple Inc.*, 583 F. Supp. 3d 769, 774-75 (W.D. Tex. 2022) ("[T]here can be no inducement or contributory infringement without an underlying act of direct infringement.") (cleaned up). K.Mizra has none.

Beyond that obvious deficiency, K.Mizra also has no evidence of intent. Induced infringement requires "knowing[] induce[ment]" of direct infringement" and "specific intent to induce that infringement." *ACQIS LLC v. Wiwynn Corp.*, 614 F. Supp. 3d 499, 503 (W.D. Tex. 2022) (cleaned up). "Willful blindness may satisfy the knowledge requirement and circumstantial evidence may suffice to prove specific intent." *Id.* (citations omitted). K.Mizra cannot possibly show this and doesn't try. Its entire intent case consists of a single conclusory sentence:

> Cisco also induces infringement of the asserted claims by (1) instructing users on how to use the Accused Products in an infringing manner; (2) providing customer support and training online and through its customer support call centers on how to use the Accused Products in an infringing manner; and (3) directing its customers to additional online sources with instructions on how to infringe the '705 Patent.

Ex. F at 1. The only cited support is to two voluminous ISE product guides.[11] K.Mizra's expert neither discusses the content of the guides nor explains how they encourage or teach Cisco customers to perform any claim limitations. The guides, for example, say nothing about setting up quarantine to skip redirection if the user has requested a remediation site, and nothing about

[11] Ex. F at 1 (citing https://ciscocustomer.lookbookhq.com/iseguidedjourney/BYOD-configuration; https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/4561-docs-security/6187/1/how-to-enable-notification-RTC_Imran_Bashir.pdf).

deploying AnyConnect with a version of Windows that requires a trusted platform module. Neither guide mentions the trusted platform module at all, or Windows 10 or 11, or AnyConnect. They do not reference, much less teach, the accused combination. Because they teach a concededly non-infringing use of ISE, the guides cannot, as a matter of law, prove the requisite intent. *Vita-Mix Corp. v. Basic Holding, Inc.*, 581 F.3d 1317, 1329 (Fed. Cir. 2009) (affirming summary judgment of no inducement). K.Mizra has identified no other evidence of inducement.

Further defeating any showing of intent, there is no evidence that Cisco instructs or encourages its customers to require their individual end users (e.g., employees) to use AnyConnect on Windows 10 or 11 laptops containing a trusted platform module. Cisco is indifferent to what operating systems its customers' employees use; they may use AnyConnect on non-accused versions of Windows, or an Apple or Linux operating system. Ex. H at 2. Cisco has no reason to care because AnyConnect works on all of those platforms, none of which even allegedly require a trusted platform module. *Id.* Thus, even if the product guides could somehow suffice as evidence of inducement regarding other elements of the claims, K.Mizra's inducement claim would still fail.

Finally, K.Mizra cannot prove contributory infringement. In addition to specific intent, § 271(c) requires the absence of substantial noninfringing uses. *Fujitsu Ltd. v. Netgear Inc.*, 620 F.3d 1321, 1326 (Fed. Cir. 2010). K.Mizra's expert report does not advance a contributory infringement theory—presumably because it is undisputed that ISE and AnyConnect at the Premier license level are sold separately; each can be used without the other; and they can be used together for purposes other than the accused posture check. Ex. C ¶99; Ex. H at 8; Ex. I (ISE Guide) at 20, 26, 33-35 (listed in Dr. Cole's Report, Ex. C, as materials considered No. 464). There is no possibility of evidence, and K.Mizra has not suggested, that the products lack a substantial

noninfringing use.[12]

C. Even assuming assembly and use, every asserted claim requires (at least) two limitations that as a matter of law the Accused Combination lacks.

Whether styled as method, system, or computer readable media claims, every asserted claim requires: (1) a TPM, and (2) DNS redirection. Neither is even arguably present.

1. ***Trusted Platform Module.*** In full, this limitation provides "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host." To satisfy the limitation, K.Mizra relies on the asserted presence of a TPM in Windows 10 and Windows 11 operating systems, and contends that AnyConnect (when used on such systems to connect to a network running ISE) calls certain Microsoft Windows routines that in turn "use random numbers generated by" a TPM. Ex. F at 38. But K.Mizra admits that source code is what determines a product's functionality, and that it has no Microsoft source code that shows those routines call a TPM. Ex. E at 18:23-19:2, 143:12-22. Nor do the excerpts of Microsoft documentation pasted into its expert's report show that the named routines call a TPM—only that they generate random numbers. Ex. F at 38, 40-41; Ex. E at 134:5-145:15.

Even K.Mizra's highly attenuated theory, namely: that AnyConnect is "associated with" a TPM because it allegedly retrieves a random number from a Microsoft routine that generates randomness using entropy to which a TPM was one of seven contributing sources, Ex. F at 40-41, lacks proof. K.Mizra's expert never explains how AnyConnect uses this random number, and *nowhere* asserts that AnyConnect's accused ISE posture feature does so. *See* Ex. F at 15-21, 31-42. Given his recognition that the claims require use of the TPM, Ex. E at 137:17-23, K.Mizra's

[12] This is another reason why K.Mizra's inducement theory fails. "Especially where a product has substantial non-infringing uses, intent to induce infringement cannot be inferred even when the defendant has actual knowledge that some users of its product may be infringing the patent." *Warner–Lambert Co. v. Apotex Corp.*, 316 F.3d 1348, 1365 (Fed. Cir. 2003).

infringement expert has not offered any opinion that, if accepted, would satisfy this limitation.

K.Mizra's validity expert set a higher bar for "associated with a TPM" in an effort to distinguish prior art. This further confirms that there is no infringement. K.Mizra's experts both recognize that a patent claim must be read the same way for infringement and validity. Ex. E at 11:4-13; Ex. D at 13:11-14:20. Yet K.Mizra's validity expert opines that the claims require the TPM to generate the posture information (the contents of the posture check report K.Mizra accuses of being an "attestation of cleanliness") and to store the cryptographic keys used to generate the digital signature applied to the attestation of cleanliness. Ex. G (Medvidovic Validity Report) ¶¶ 194, 210; Ex. D at 91:10-25, 99:6-10. These TPM functions, he said, are "at the heart of this [the '705] invention." Ex. D at 91:16-25. K.Mizra's infringement expert did not opine that the accused TPM generates the cleanliness attestation or the keys used to sign it; his modest assertions, even if supported, would not come close to meeting the validity expert's requirements for "associated with" a TPM. The scope K.Mizra's validity expert applied precludes infringement. "[A] patent may not, like a 'nose of wax,' be twisted one way to avoid anticipation and another to find infringement." *ESW Holdings, Inc. v. Roku, Inc.*, No. 6-19-CV-00044-ADA, 2021 WL 3742201, at *5 (W.D. Tex. Aug. 24, 2021) (quoting *Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1351 (Fed. Cir. 2001)).

2. ***DNS Redirect.*** When the response lacks a valid digitally signed attestation of cleanliness, every asserted claim requires quarantining the computer attempting to access the network in a specific way—by using a DNS redirect, which returns the IP address of the quarantine server instead of the IP address for the requested URL.[13] K.Mizra has not and cannot point to a

[13] "…in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server…" Ex. A at cl. 1, 20:14-17, cl. 12, 21:27-30, cl. 19, 22:41-43. An IP address is a number that uniquely identifies a host's network interface, formatted as, for example,

DNS redirect in the accused products because the accused Cisco products do not employ that method of redirection. Instead, Cisco uses URL or HTTP redirect, in which the requester is instructed to ask for a different URL. K.Mizra's infringement report shows only a URL redirect; nothing shows a DNS redirect. Ex. F at 68 [redacted] 71 [redacted], 73 (step 5, [redacted] Ex. E at 200:23-202:23, 199:20-200:5 (URL redirect is shown in report; expert could not recall seeing DNS redirect in the code).

The two forms of redirect are distinct and not equivalent, as K.Mizra's validity expert admits. Ex. D at 123:7-9 [redacted] 126:1-6 [redacted] In any case, K.Mizra has not asserted equivalence, and the patent examiner identified the DNS redirect feature as a reason for allowance of the '705 Patent, precluding any equivalence argument. Ex. J ('705 Prosecution History) at MIZCIS00002950 ("The closest prior art … disclose detecting abnormal events on host, and redirecting to quarantine serve to get remediated; however, they fail to anticipate or render serving both the specific quarantine notification page *with the DNS redirection* when in combination with the remaining claim limitations." (emphasis added)). K.Mizra has pointed to no evidence that the accused products use a DNS redirect.

V. CONCLUSION

Cisco respectfully asks the Court to grant summary judgment of noninfringement.

192.168.1.45. A DNS query is a request to a domain name server to provide the IP address that corresponds to a particular hostname, typically a web address or "URL" (e.g., www.google.com). Ex. B ¶ 96.

Dated: June 9, 2023

Respectfully submitted,

By: */s/ Melissa R. Smith*

Melissa R. Smith (State Bar No. 24001351)
melissa@gillamsmithlaw.com
GILLAM & SMITH LLP
303 South Washington Avenue
Marshall, TX 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257

Elizabeth R. Brannen (*Pro Hac Vice*)
ebrannen@stris.com
Kenneth J. Halpern (*Pro Hac Vice*)
khalpern@stris.com
Sarah Rahimi *(Pro Hac Vice)*
srahimi@stris.com
STRIS & MAHER LLP
777 S. Figueroa St, Ste 3850
Los Angeles, CA 90017
Telephone: (213) 995-6800
Facsimile: (213) 216-0299

Jhaniel James *(Pro Hac Vice)*
jjames@stris.com
STRIS & MAHER LLP
111 N Calhoun St, Ste 10
Tallahassee, FL 32301
Telephone: (213) 995-6800
Facsimile: (813) 330-3176

Attorneys for Defendant
Cisco Systems, Inc.

CERTIFICATE OF SERVICE

I certify that on June 9, 2023, the documents filed with the Clerk of Court via the Court's CM/ECF system under seal in the above-captioned case were subsequently served on all counsel of record by electronic mail.

/s/ Melissa R. Smith